US 20180040220A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2018/0040220 A1**

Landauer et al. (43) **Pub. Date: Feb. 8, 2018**

(54) **ELECTRONIC TAMPER DETECTION DEVICE**

(71) Applicant: **NXP B.V.**, Eindhoven (NL)

(72) Inventors: **Gerhard Martin Landauer**, Gratkorn (AT); **Ivan Jesus Rebollo Pimentel**, Gratkorn (AT)

(21) Appl. No.: **15/667,602**

(22) Filed: **Aug. 2, 2017**

(30) **Foreign Application Priority Data**

Aug. 2, 2016 (EP) 16182327.3

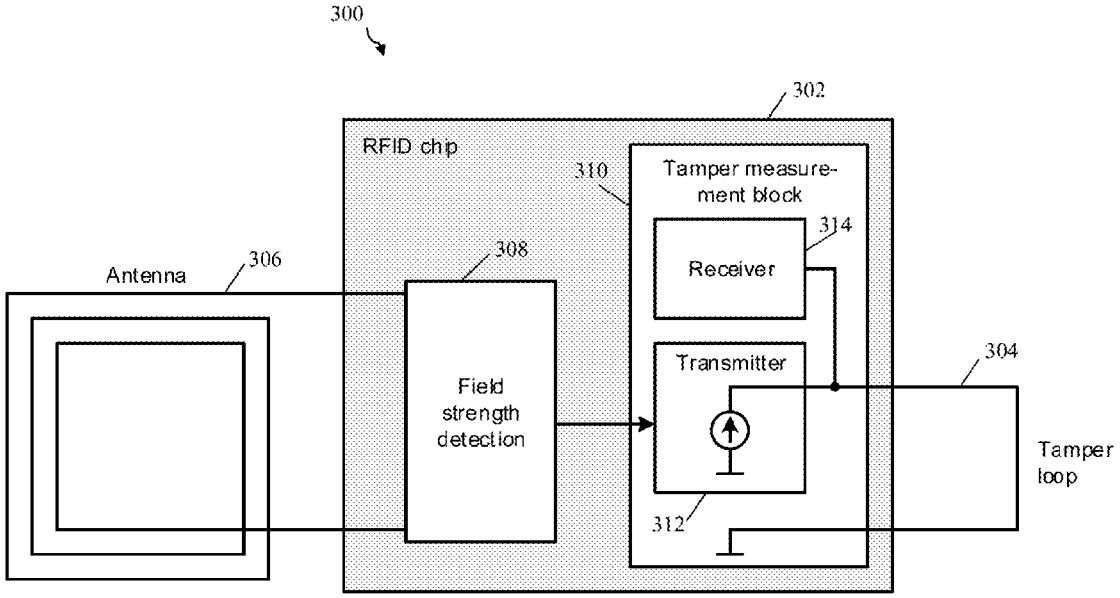
Publication Classification

(51) **Int. Cl.**
G08B 13/24 (2006.01)

(52) **U.S. Cl.**
CPC ***G08B 13/2417*** (2013.01)

(57) **ABSTRACT**

According to a first aspect of the present disclosure, an electronic tamper detection device is provided, comprising a radio frequency antenna, a tamper loop, a power level determination unit and a tamper measurement unit, wherein: the power level determination unit is configured to determine a power level of the tamper detection device; the tamper measurement unit is configured to generate a measurement signal and to transmit said measurement signal through the tamper loop; the tamper measurement unit is further configured to adapt the measurement signal in dependence on the power level. According to a second aspect of the present disclosure, a corresponding tamper detection method is conceived. According to a third aspect of the present disclosure, a corresponding non-transitory computer-readable storage medium comprising instructions is provided.



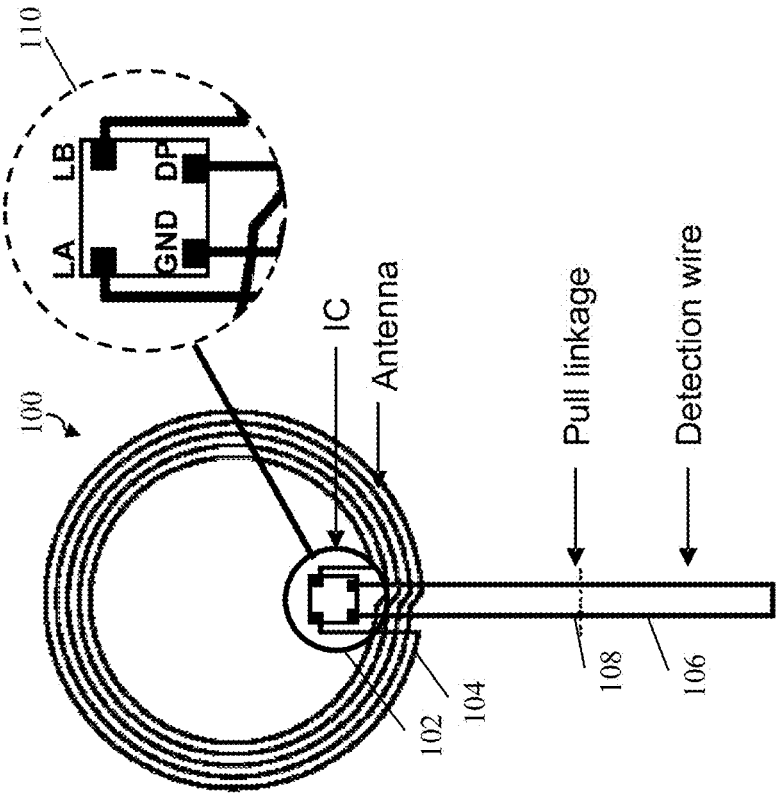

110
LB
DP
LA
GND
100
IC
Antenna
Pull linkage
Detection wire
102
104
108
106

FIG. 1

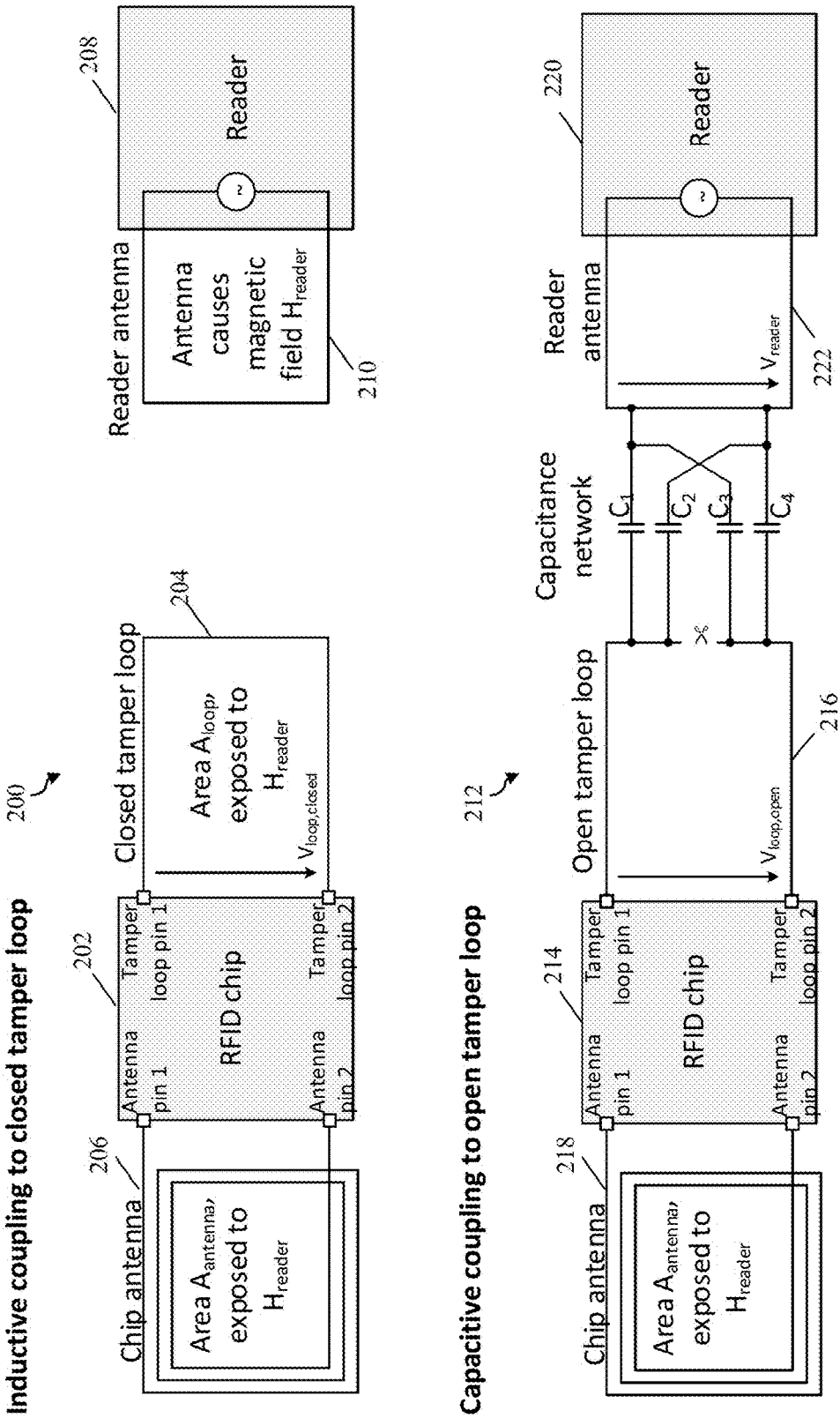

Inductive coupling to closed tamper loop
206
Chip antenna
Area $A_{antenna}$, exposed to H_{reader}
202
Antenna pin 1
Tamper loop pin 1
RFID chip
Antenna pin 2
Tamper loop pin 2
Closed tamper loop
204
Area A_{loop}, exposed to H_{reader}
$V_{loop,closed}$
Reader antenna
Antenna causes magnetic field H_{reader}
210
208
Reader
Capacitive coupling to open tamper loop
212
218
Chip antenna
Area $A_{antenna}$, exposed to H_{reader}
214
Antenna pin 1
Tamper loop pin 1
RFID chip
Antenna pin 2
Tamper loop pin 2
Open tamper loop
216
$V_{loop,open}$
Capacitance network
C_1
C_2
C_3
C_4
Reader antenna
V_{reader}
222
220
Reader

FIG. 2

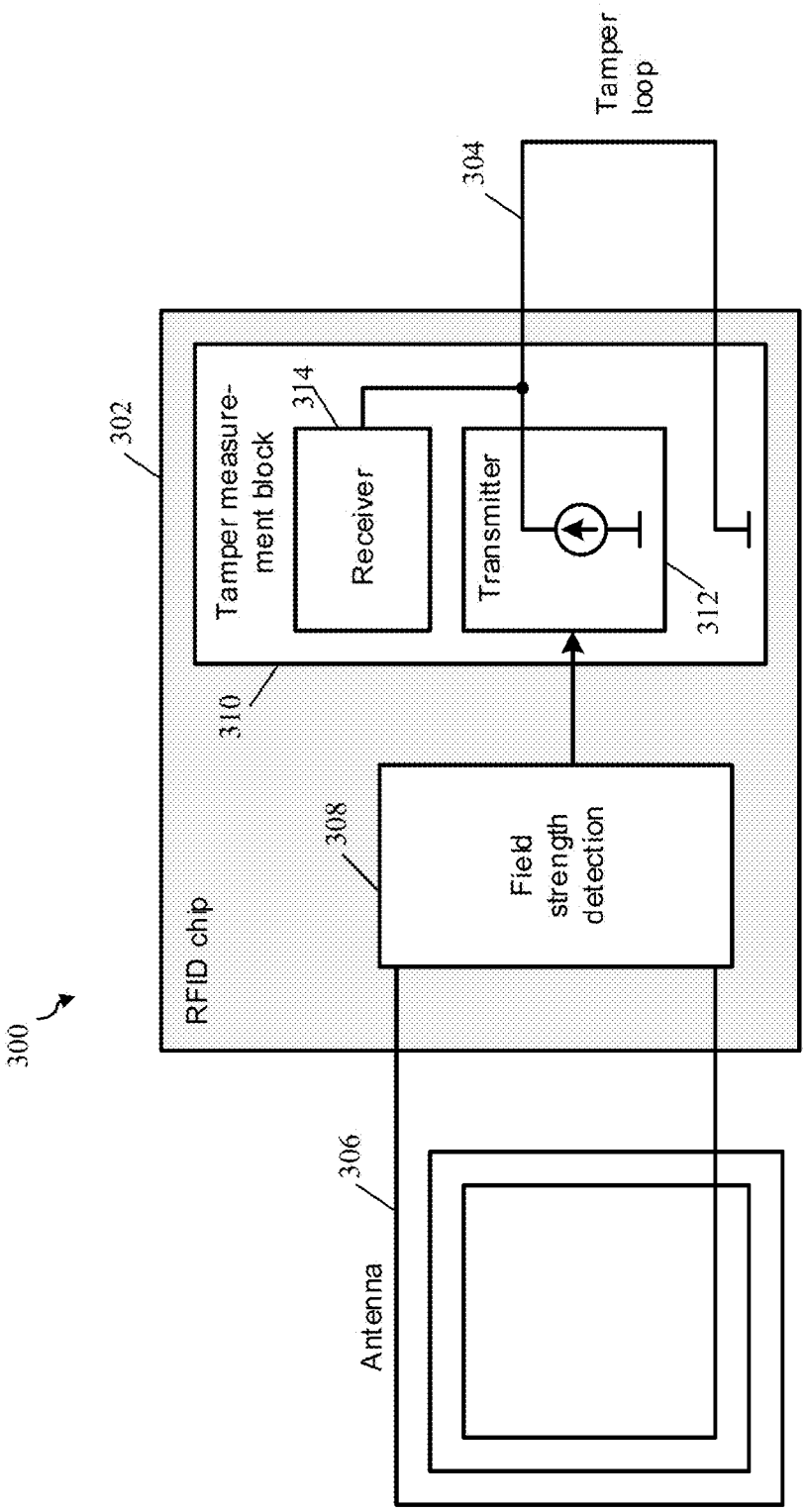

300
RFID chip
302
Tamper measure-ment block
310
Receiver
314
Transmitter
312
304
Tamper loop
308
Field strength detection
306
Antenna

FIG. 3A

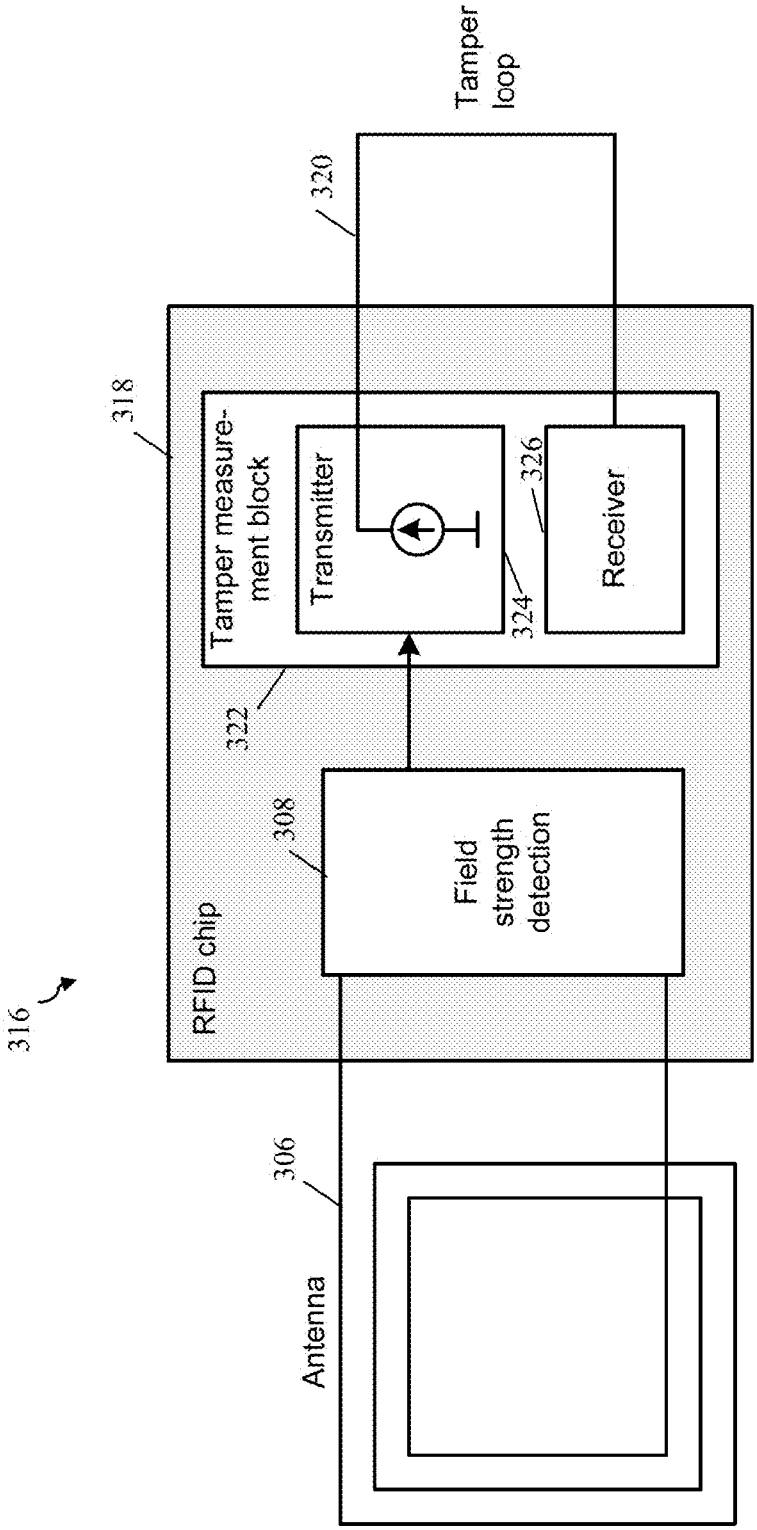

316
RFID chip
318
Tamper measure-ment block
Transmitter
Receiver
Field strength detection
Antenna
Tamper loop
306
308
320
322
324
326

FIG. 3B

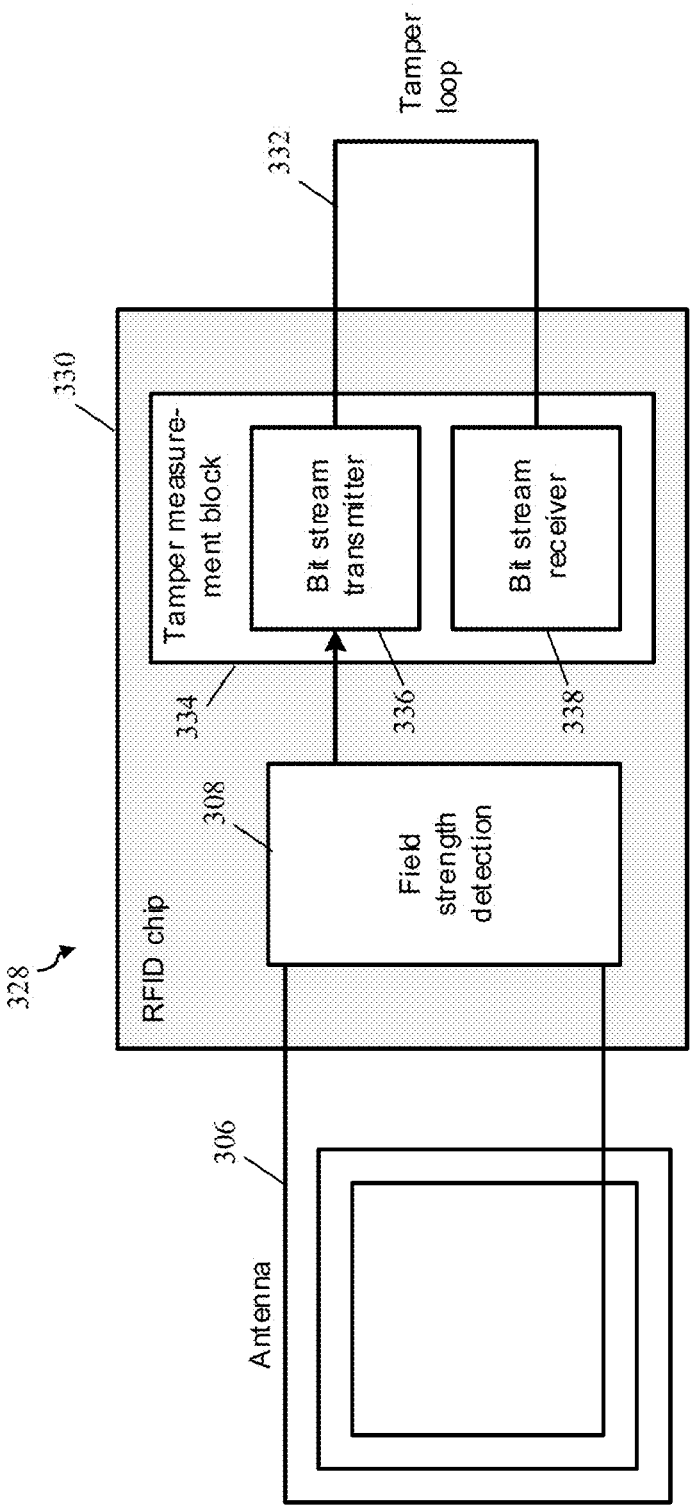

Tamper loop
332
330
Tamper measure-ment block
Bit stream transmitter
Bit stream receiver
334
336
338
308
Field strength detection
RFID chip
328
306
Antenna

FIG. 3C

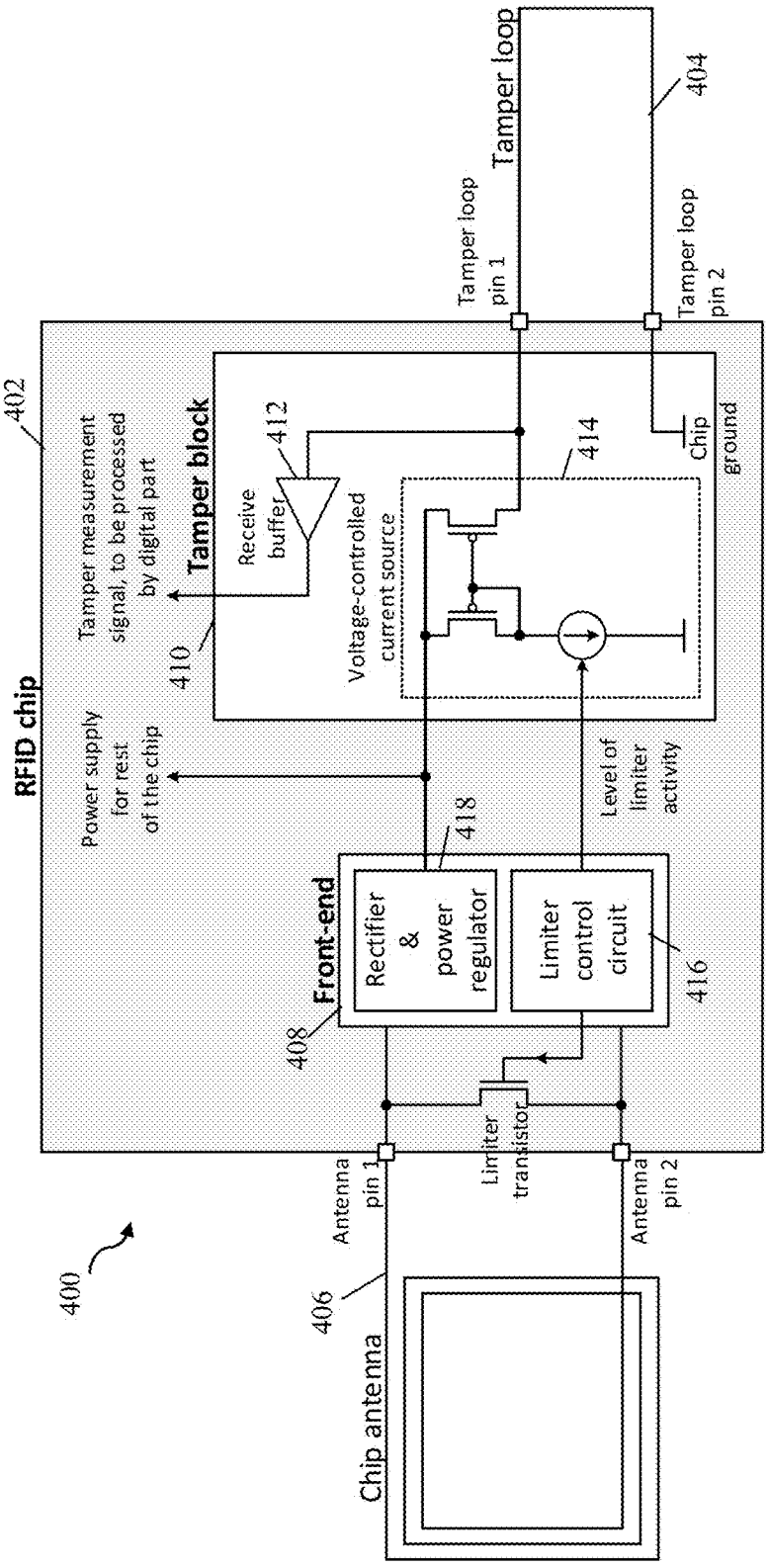

400
402
RFID chip
Tamper measurement signal, to be processed by digital part
Tamper block
412
Receive buffer
410
Voltage-controlled current source
414
Tamper loop
404
Tamper loop pin 1
Tamper loop pin 2
Chip ground
Power supply for rest of the chip
Level of limiter activity
418
Front-end
408
Rectifier & power regulator
Limiter control circuit
416
Limiter transistor
Antenna pin 1
Antenna pin 2
406
Chip antenna

FIG. 4

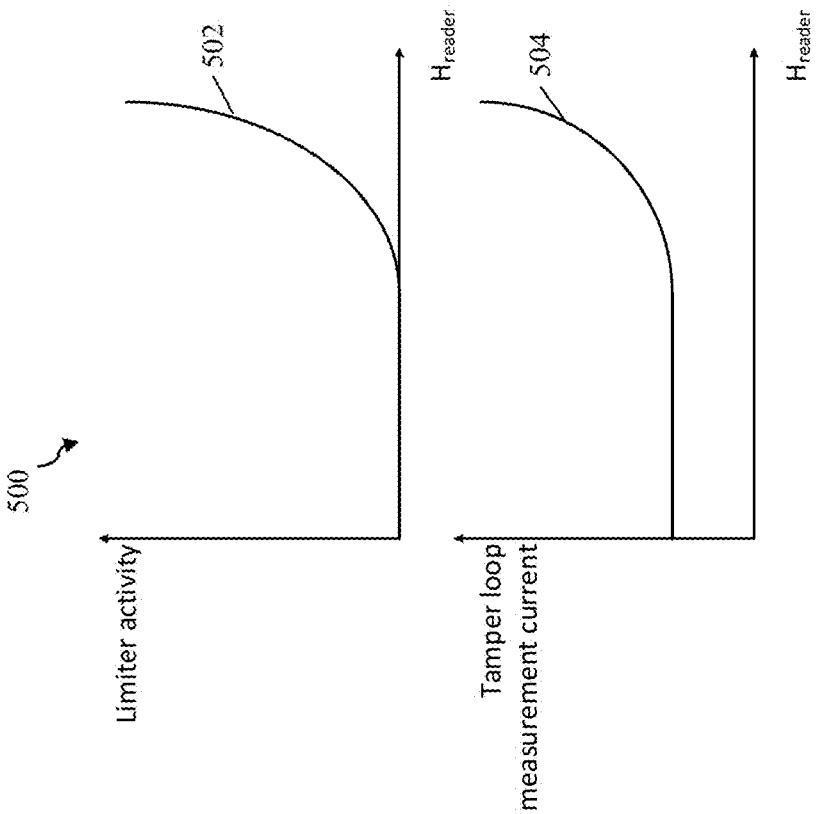

500
502
504
H_{reader}
H_{reader}
Limiter activity
Tamper loop measurement current

FIG. 5

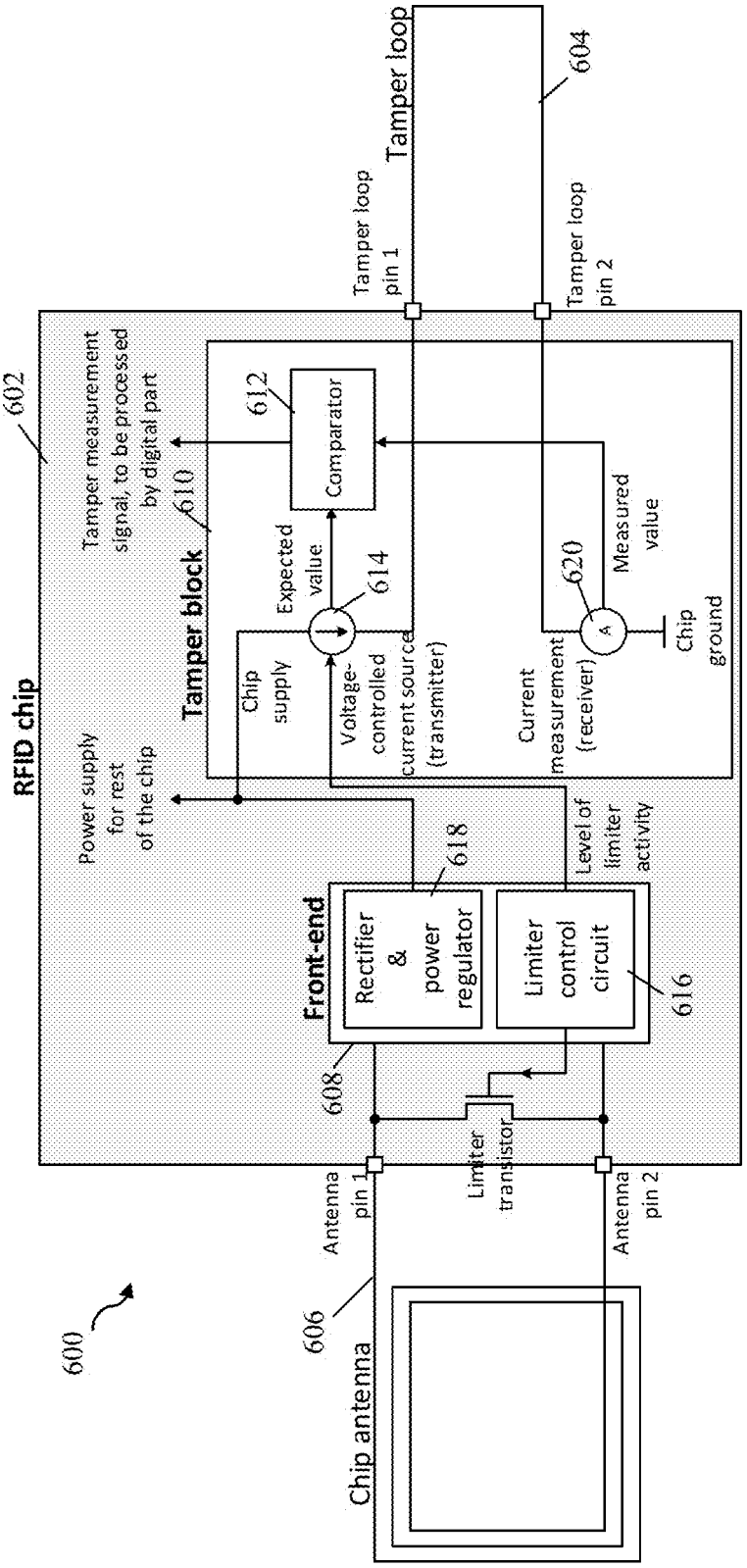

600
602
RFID chip
Power supply for rest of the chip
Tamper measurement signal, to be processed by digital part
610
Tamper block
Chip supply
Expected value
614
Voltage-controlled current source (transmitter)
612
Comparator
Current measurement (receiver)
620
Measured value
Chip ground
Tamper loop pin 1
Tamper loop pin 2
Tamper loop
604
Front-end
Rectifier & power regulator
618
Limiter control circuit
616
Level of limiter activity
608
Limiter transistor
Antenna pin 1
Antenna pin 2
606
Chip antenna

FIG. 6

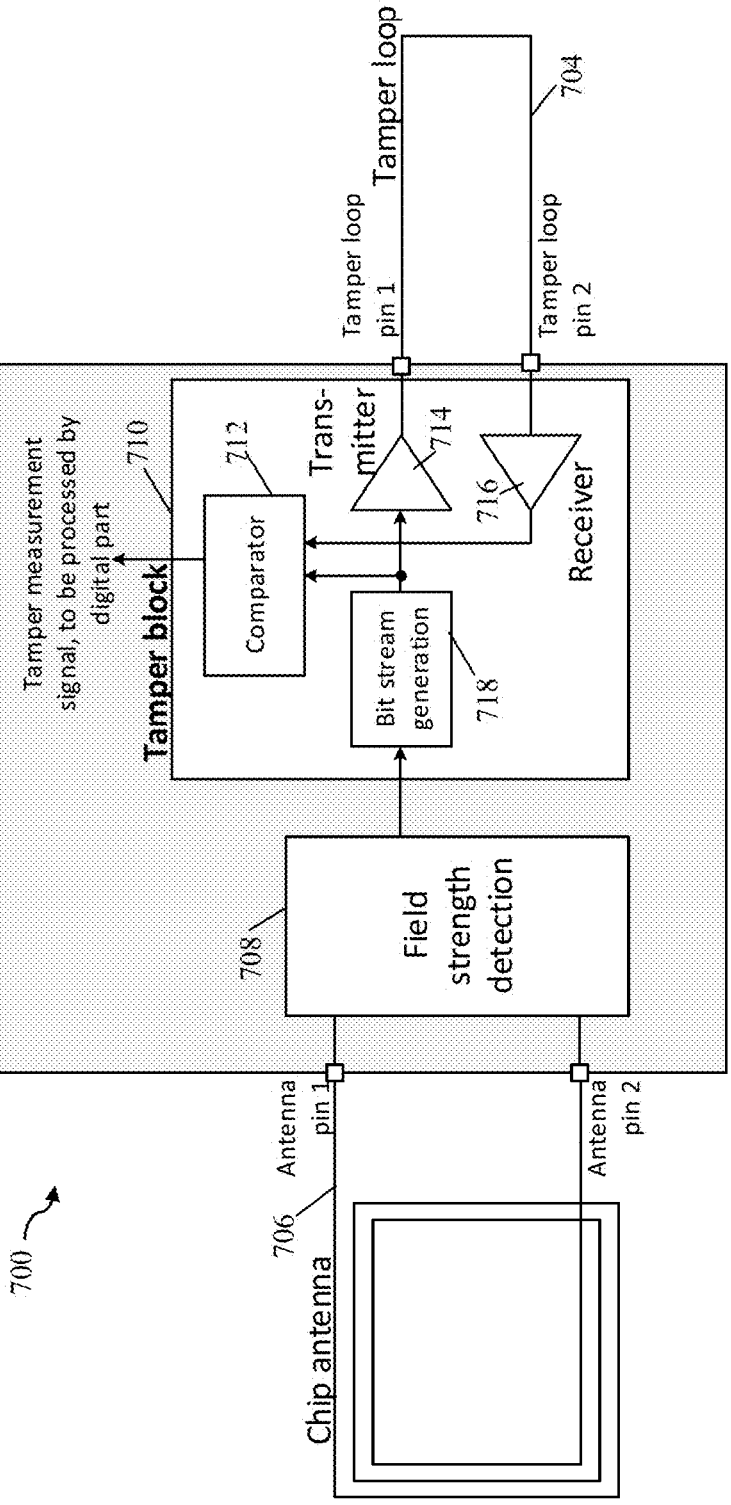

700
RFID chip
702
Tamper measurement signal, to be processed by digital part
710
Tamper block
712
Comparator
Trans-mitter
714
716
Receiver
Bit stream generation
718
Field strength detection
708
Tamper loop
Tamper loop pin 1
Tamper loop pin 2
704
Antenna pin 1
Antenna pin 2
706
Chip antenna

FIG. 7

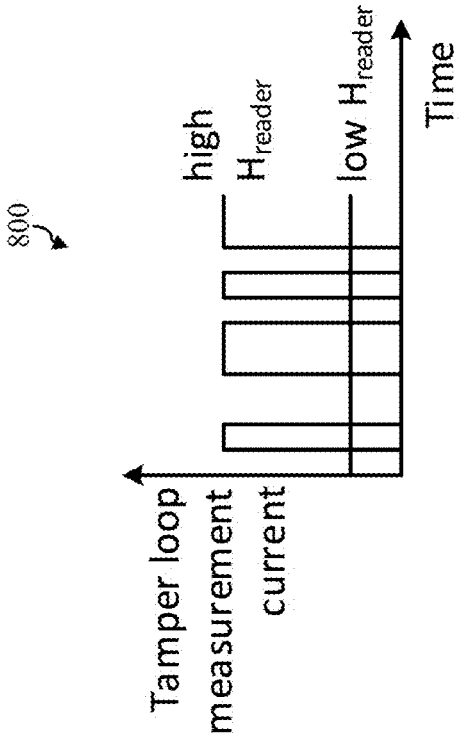

800
Tamper loop measurement current
high H_{reader}
low H_{reader}
Time

FIG. 8

ELECTRONIC TAMPER DETECTION DEVICE

FIELD

[0001] The present disclosure relates to an electronic tamper detection device. Furthermore, the present disclosure relates to a corresponding tamper detection method, and to a corresponding non-transitory computer-readable storage medium comprising instructions.

BACKGROUND

[0002] Electronic tamper detection devices may be used to detect tampering with closed or sealed products, such as bottles, packets and other containers. For example, in the spirits industry and the pharmaceutical industry such tamper detection devices may be useful. Tamper detection devices often contain a so-called tamper loop. A tamper loop may for example comprise a conductive wire that is broken when a closure or seal in which it is concealed is broken. Frequently used tamper detection devices are radio frequency identification (RFID) or near field communication (NFC) tags comprising or extended with a tamper loop. It may be desirable to improve these tamper detection devices, so that tamper attempts can be detected with a higher degree of reliability while not overloading the often weak electrical power supply of such devices.

SUMMARY

[0003] According to a first aspect of the present disclosure, an electronic tamper detection device is provided, comprising a radio frequency antenna, a tamper loop, a power level determination unit and a tamper measurement unit, wherein: the power level determination unit is configured to determine a power level of the tamper detection device; the tamper measurement unit is configured to generate a measurement signal and to transmit said measurement signal through the tamper loop; the tamper measurement unit is further configured to adapt the measurement signal in dependence on the power level.

[0004] In one or more embodiments, the power level corresponds to the strength of a radio frequency field present on the radio frequency antenna and the power level determination unit is configured to detect said strength, or the power level corresponds to a chip supply voltage and the power level determination unit is configured to monitor said chip supply voltage.

[0005] In one or more embodiments, the tamper measurement unit is further configured to receive the measurement signal from the tamper loop or to receive a signal derived from the measurement signal from the tamper loop.

[0006] In one or more embodiments, the tamper measurement unit is configured to change the magnitude of the measurement signal in response to a change of the power level.

[0007] In one or more embodiments, the field strength detection unit comprises a limiter control circuit operatively coupled to the tamper measurement unit, and the tamper measurement unit is configured to change the magnitude of the measurement signal under control of the limiter control circuit.

[0008] In one or more embodiments, the tamper measurement unit is configured to change the waveform of the measurement signal in response to a change of the power level.

[0009] In one or more embodiments, the waveform of the measurement signal is a complex waveform, in particular a waveform that represents a bit stream, if the power level exceeds a predefined threshold.

[0010] In one or more embodiments, the waveform of the measurement signal represents a constant current if the power level does not exceed said threshold.

[0011] In one or more embodiments, the device is an RFID-enabled tamper detection device.

[0012] In one or more embodiments, the device is a BLE-enabled tamper detection device.

[0013] In one or more embodiments, the tamper measurement unit comprises a voltage-controlled current source, a current-controlled current source, a current-controlled voltage source, or a voltage-controlled voltage source.

[0014] In one or more embodiments, the tamper loop is a conductive wire.

[0015] In one or more embodiments, the tamper measurement unit is configured to generate a tamper measurement signal for further processing by a digital circuit.

[0016] According to a second aspect of the present disclosure, a tamper detection method using an electronic tamper detection device is conceived, wherein said device comprises a radio frequency antenna, a tamper loop, a power level determination unit and a tamper measurement unit, the method comprising: the power level determination unit determines a power level of the tamper detection device; the tamper measurement unit generates a measurement signal and transmits said measurement signal through the tamper loop; the tamper measurement unit adapts the measurement signal in dependence on the power level.

[0017] According to a third aspect of the present disclosure, a non-transitory computer-readable storage medium is provided, comprising instructions which, when executed by a processing unit, carry out or control a method of the kind set forth.

DESCRIPTION OF DRAWINGS

[0018] Embodiments will be described in more detail with reference to the appended drawings, in which:

[0019] FIG. **1** shows an example of a tamper detection device;

[0020] FIG. **2** shows examples of RFID systems and of disturbances coupled to their tamper loops;

[0021] FIG. **3**A shows an illustrative embodiment of a tamper detection device;

[0022] FIG. **3**B shows another illustrative embodiment of a tamper detection device;

[0023] FIG. **3**C shows a further illustrative embodiment of a tamper detection device;

[0024] FIG. **4** shows a further illustrative embodiment of a tamper detection device:

[0025] FIG. **5** shows a relationship between limiter activity and tamper loop measurement current;

[0026] FIG. **6** shows a further illustrative embodiment of a tamper detection device;

[0027] FIG. **7** shows a further illustrative embodiment of a tamper detection device;

[0028] FIG. **8** shows a relationship between tamper loop measurement current and time in the embodiment shown in FIG. **7**.

DESCRIPTION OF EMBODIMENTS

[0029] FIG. **1** shows an example of an electronic tamper detection device **100**. In this example, the tamper detection device **100** is an RFID or NFC tag equipped with a tamper loop. The tag may be a so-called passive tag, i.e. a tag powered by an electromagnetic field generated by an external device (not shown). The tag comprises an integrated circuit **102** (i.e., a tag circuit or "chip") which is coupled through contact pads LA and LB to an antenna **104** for establishing wireless communication with said external device. The tamper loop is formed by a detection wire **106** (i.e., a conductive wire) which is coupled to the integrated circuit **102** through contact pads GND and DP. The detection wire **106** may for example be concealed in a closure comprising a pull linkage **108**. In operation, once the detection wire **106** (tamper loop) has been broken (e.g., at the pull linkage **108**) and the tag is powered by said electromagnetic field, the tag can detect that the detection wire **106** has been broken and act accordingly.

[0030] Thus, in the tamper detection device **100** shown in FIG. **1**, there is, in addition to the radio frequency (RF) antenna that provides the chip **102** with power and that is used for communication with an external device, a tamper loop **106** which may be broken in a tamper attempt (e.g., by manipulating the closure of a bottle). The open/closed status of this loop can be detected by the RFID chip **102** and communicated to a reader (not shown). While the tag shown in FIG. **1** operates in the high-frequency (HF) band or range, tags supplied by a low-frequency (LF) or ultra-high frequency (UHF) field may also be equipped with a tamper loop of the kind set forth.

[0031] Examples of RFID devices equipped with tamper loops have been described in US 2013/0135104 A1, U.S. Pat. No. 6,888,509 B2, and US 2012/0218110 A1. Passive RFID tags should be very energy-efficient as they should be able to function when they are supplied by weak fields. This requires also the tamper measurement to be energy-efficient, i.e. the measurement current to be low, and in consequence the measurement result is susceptible to disturbances from the field. The difference between the minimum and maximum field strength at which the chip **102** must function can yet be in the range of several decades. In some examples there is not only an energy transfer from the field to the tag's antenna **104**, but also an unwanted coupling to the tamper loop **106**. That is to say, when the chip **102** is exposed to high field strengths and a measurement of the status of the tamper loop **106** is done, this coupling may lead to a disturbance of the measurement signal and therefore to false detections (i.e., the chip **102** detects an open tamper loop **106**, although the loop **106** is closed) or to false non-detections (i.e., the chip **102** detects a closed tamper loop **106**, although the loop **106** is open). Improvements that are energy-efficient and robust against disturbances of the measurement signal will now be discussed.

[0032] FIG. **2** shows examples of RFID systems **200**, **212** and of disturbances coupled to their tamper loops. In particular, it shows examples of RFID systems **200**, **212** in which disturbances of a tamper measurement signal may occur. When a passive RFID tag with a tamper loop is powered by a reader, then not only the chip antenna, but unfortunately also the tamper loop is exposed to the RF field and therefore the tamper measurement can be disturbed by the field. In HF operation two types of disturbances can be distinguished. A first type of disturbance is shown in the upper part of FIG. **2**; this type of disturbance may occur when an RFID system **200** uses inductive coupling. In particular, when a reader **208** provides a magnetic field H_{reader} which induces a voltage $V_{loop,closed}$ in the closed tamper loop **204**, then $V_{loop,closed}$ is proportional to $A_{loop}*H_{reader}$ and therefore a large tamper loop or a strong field can cause a high voltage that results in a wrong tamper measurement (i.e., a false detection: the tamper loop **204** seems open although it is closed). Restricting A_{loop} or H_{reader} mitigates this problem, but such restrictions may not be possible in a final product. A second type of disturbance is shown in the lower part of FIG. **2**; this type of disturbance may occur when the open tamper loop **216** of an RFID system **212** is exposed to capacitive coupling to the reader antenna **222**. In particular, in case of an open tamper loop **216** a potential difference V_{reader} between two zones of the reader antenna **222** can be capacitively coupled to the two remaining wires of the tamper loop **216** and cause a voltage $V_{loop,open}$. A strong capacitive coupling or a high voltage at the reader antenna **222** can cause a wrong tamper measurement (i.e. a false non-detection: the tamper loop **216** seems closed although it is open). It is noted that the coupling behavior of a UHF tag is different. For instance, a UHF tag antenna is not a loop antenna but a dipole antenna and an open tamper loop may also act as such a dipole antenna receiving energy from the radiative field. However, it still occurs that a stronger field provides the chip with more energy but also exposes the tamper loop to more disturbances.

[0033] Therefore, in accordance with the present disclosure, an electronic tamper detection device is provided, comprising a radio frequency antenna, a tamper loop, a power level determination unit and a tamper measurement unit. The power level determination unit is configured to detect a power level of the tamper detection device. The tamper measurement unit is configured to generate a measurement signal and to transmit said measurement signal through the tamper loop. Furthermore, the tamper measurement unit is configured to adapt the measurement signal in dependence on the power level. In this way, the tamper measurement robustness may be made dependent on the availability of energy. For example, the power level determination unit may detect the strength of the RF field present on the antenna, and when the field is weak, the amount of available energy is low, but also disturbances are low, so a simple and energy-efficient tamper measurement can be performed. Furthermore, when the field is strong, disturbances are high, but the amount of available energy is also high, so a more complex and less energy-efficient tamper measurement can be performed. It is noted that, although the presently disclosed device and method are described in the context of RFID systems, their application is not limited thereto. The presently disclosed device and method may also be applied to advantage in other types of communication systems, such as Bluetooth Low Energy (BLE) systems and other low-power wireless communication systems. In that case, the tamper detection device may be a BLE-enabled tamper detection device, for example.

[0034] In one or more embodiments, the power level corresponds to the strength of a radio frequency field present

on the radio frequency antenna and the power level determination unit is configured to detect said strength. Alternatively, the power level corresponds to a chip supply voltage and the power level determination unit is configured to monitor said chip supply voltage. More specifically, the power level determination unit may detect the strength of the RF field directly, or it may monitor the chip supply voltage which is dependent on the strength of the RF field.

[0035] In one or more embodiments, the tamper measurement unit is further configured to receive the measurement signal from the tamper loop or to receive a signal derived from the measurement signal from the tamper loop. More specifically, in a practical and efficient implementation, the tamper measurement unit also contains a receiver for the measurement signal itself (e.g., measurement current is injected on one side of the loop and received on other side of the loop) or a signal derived from the measurement signal (e.g., measurement current is injected on one side of the loop and the resulting voltage is received on the same side of the loop).

[0036] In one or more embodiments, the tamper measurement unit is configured to change the magnitude of the measurement signal in response to a change of the power level. In this way, a practical and efficient implementation may be realized. For example, in case the power level corresponds to the strength of the RF field, the measurement current may be monotonically dependent on the detected strength of the RF field.

[0037] FIG. **3**A shows an illustrative embodiment of a tamper detection device **300**. The tamper detection device **300** comprises an RFID chip **302** operatively coupled to an RF antenna **306**. More specifically, the RF antenna **306** is coupled to a field strength detection unit **308** comprised in the RFID chip **302**. Furthermore, the tamper detection device **300** comprises a tamper loop **304** operatively coupled to the RFID chip **302**. More specifically, the tamper loop **304** is coupled to a transmitter **312** and receiver **314** in a tamper measurement block **310** of the RFID chip **302**. In operation, the field strength detection unit **308** detects the strength of the RF field present on the antenna **306**. Furthermore, the transmitter **312** adjusts the measurement current in dependence on the field strength detected by the field strength detection unit **308**. This embodiment enables a stronger measurement current (and therefore a more robust measurement) when a stronger field is available. In this way, the probability of false non-detections may be reduced. A detailed implementation of this embodiment is shown in FIG. **4**.

[0038] FIG. **3**B shows another illustrative embodiment of a tamper detection device **316**. The tamper detection device **316** comprises an RFID chip **318** operatively coupled to an RF antenna **306**. More specifically, the RF antenna **306** is coupled to a field strength detection unit **308** comprised in the RFID chip **318**. Furthermore, the tamper detection device **316** comprises a tamper loop **320** operatively coupled to the RFID chip **318**. More specifically, the tamper loop **320** is coupled between a transmitter **324** and receiver **326** in a tamper measurement block **322** of the RFID chip **302**. In operation, the field strength detection unit **308** detects the strength of the RF field present on the antenna **306**. Furthermore, the transmitter **324** adjusts the measurement current in dependence on the field strength detected by the field strength detection unit **308**. This embodiment also enables a stronger measurement current (and therefore a more robust measurement) when a stronger field is available. In this way, the probability of false detections and the probability of false non-detections may be reduced. A detailed implementation of this embodiment is shown in FIG. **6**.

[0039] FIG. **3**C shows a further illustrative embodiment of a tamper detection device **328**. The tamper detection device **328** comprises an RFID chip **330** operatively coupled to an RF antenna **306**. More specifically, the RF antenna **306** is coupled to a field strength detection unit **308** comprised in the RFID chip **330**. Furthermore, the tamper detection device **328** comprises a tamper loop **332** operatively coupled to the RFID chip **330**. More specifically, the tamper loop **332** is coupled between a bit stream transmitter **336** and a bit stream receiver **338** in a tamper measurement block **334** of the RFID chip **330**. In operation, the field strength detection unit **308** detects the strength of the RF field present on the antenna **306**. Furthermore, the bit stream transmitter **336** may transmit a bit stream corresponding to a complex waveform through the tamper loop **332** if the strength of the RF field exceeds a predefined threshold. Furthermore, the bit stream receiver **338** may receive the bit stream transmitted through the tamper loop **332** and verify if the bit stream is unaltered, for example within a given error margin. This embodiment may prevent false non-detections when the field is sufficiently strong to allow digital patterns to be sent. A detailed implementation of this embodiment is shown in FIG. **7**.

[0040] FIG. **4** shows another illustrative embodiment of a tamper detection device **400**. In particular, FIG. **4** shows a detailed implementation of the embodiment shown in FIG. **3**A. The tamper detection device **400** comprises an RFID chip **402** which is operatively coupled to a chip antenna **406** (i.e., an RF antenna) through antenna pins. Furthermore, the tamper detection device **400** comprises a tamper loop **404** which is operatively coupled to the RFID chip **402** through tamper loop pins. In particular, the tamper loop **404** is coupled to a tamper block **410** (i.e., a tamper measurement block). Furthermore, the chip antenna **406** is coupled to a front-end **408** of the RFID chip **402**. The front-end **408** comprises a rectifier and power regulator **418** and a limiter control circuit **416**. The tamper block **410** comprises a voltage-controlled current source **414**, a receive buffer **412** and a connection to ground. In operation, the tamper block **410** may output a tamper measurement signal to be processed by one or more digital components (not shown) of the RFID chip **402**. Furthermore, the rectifier and power regulator **418** may act as a power supply for other components (not shown) of the RFID chip **402**. In this embodiment, the front-end **408** acts both as a power supply for generating the tamper measurement current and as a field strength detection unit. In particular, rectifier and power regulator **418** supplies power to the voltage-controlled current source **414** so that the latter may transmit a tamper measurement current through the tamper loop **404**. Furthermore, the limiter control circuit **416** may detect the strength of the RF field present on the chip antenna **406** and output a voltage to control the current generated by the voltage-controlled current source **414** of the tamper block **410**. Thus, the limiter control circuit **416** facilitates controlling the tamper measurement current in dependence on the strength of the RF field. Furthermore, the use of a voltage-controlled current source **414** in the tamper block **410** results in a practical and efficient implementation. Alternatively, the measurement signal could be a voltage and it could also be controlled by

a current. Thus, the tamper measurement unit may also comprise a current-controlled current source, a current-controlled voltage source, or a voltage-controlled voltage source.

[0041] Thus, FIG. **4** shows a possible implementation of an RFID tag with robust tamper functionality. The robustness is obtained by a field-strength-dependent increase of the tamper measurement current that is injected into the tamper loop **404** by a voltage-controlled current source **414**. In case of an open tamper loop a high measurement current helps to reliably overcome capacitive coupling from a reader antenna and to pull the tamper loop pin **1** to a "high" level, which is then communicated to a digital part of the RFID chip **402** as a tamper measurement signal indicative of "loop open" information. Thus, this implementation mitigates the risk of false non-detections.

[0042] Furthermore, a typical implementation of an RFID tag contains a limiter transistor, which avoids an overvoltage at the chip antenna pins in case of a strong reader field H_{reader}. The limiter transistor is gradually switched on when H_{reader} increases and the level of limiter activity indicates if there is sufficient power available to increase the tamper measurement current. Therefore, the limiter control circuit **416** can be used not only to control the limiter transistor, but also the strength of the tamper measurement current. In this way, the tamper measurement current control may be implemented in an efficient yet reliable way. In a practical and efficient implementation, the tamper loop **404** is a conductive wire through which the tamper measurement current is transmitted.

[0043] FIG. **5** shows a relationship **500** between limiter activity **502** and tamper loop measurement current **504**. In this example, which is based on the embodiment shown in FIG. **4**, the tamper loop measurement current **504** (i.e., the tamper measurement current) is a function of the limiter activity **502**. In this particular example, the tamper loop measurement current **504** increases in a similar way as the limiter activity **502**. The skilled person will appreciate that the exact relation between the tamper loop measurement current **504** and the limiter activity **502** depends on the individual application.

[0044] A possibility to allow a higher tamper measurement current when a stronger field is available is to directly observe the internal chip supply voltage (i.e., the output of the rectifier and power regulator **418**) instead of the limiter activity level. As long as the chip supply voltage is at the nominal value, a high tamper measurement current is allowed. When the RF field on the chip antenna **406** is weak, a high tamper measurement current would cause a drop of the chip supply, which can be avoided by a regulator loop that monitors the chip supply voltage and decreases the tamper measurement current as soon as it detects a drop of that voltage.

[0045] FIG. **6** shows yet another illustrative embodiment of a tamper detection device **600**. In particular, FIG. **6** shows a detailed implementation of the embodiment shown in FIG. **3**B. The tamper detection device **600** comprises an RFID chip **602** which is operatively coupled to a chip antenna **606** (i.e., an RF antenna) through antenna pins. Furthermore, the tamper detection device **600** comprises a tamper loop **604** which is operatively coupled to the RFID chip **602** through tamper loop pins. In particular, the tamper loop **604** is coupled to a tamper block **610** (i.e., a tamper measurement block). Furthermore, the chip antenna **606** is coupled to a front-end **608** of the RFID chip **602**. The front-end **608** comprises a rectifier and power regulator **618** and a limiter control circuit **616**. The tamper block **610** comprises a voltage-controlled current source **614**, a comparator **612** and a measurement current receiver **620** that is connected to ground. In operation, the tamper block **610** may output a tamper measurement signal to be processed by one or more digital components (not shown) of the RFID chip **602**. Furthermore, the rectifier and power regulator **618** may act as a power supply for other components (not shown) of the RFID chip **602**. In this embodiment, the front-end **608** acts both as a power supply for generating the tamper measurement current and as a field strength detection unit. In particular, rectifier and power regulator **618** supplies power to the voltage-controlled current source **614** so that the latter may transmit a tamper measurement current through the tamper loop **604**. Furthermore, the limiter control circuit **616** may detect the strength of the RF field present on the chip antenna **606** and output a voltage to control the current generated by the voltage-controlled current source **614** of the tamper block **610**. The comparator **612** compares an expected value of the received tamper measurement current, output by the voltage-controlled current source **614**, with the current received by the receiver **620**. If the received current substantially matches the expected value, the comparator **612** outputs a tamper measurement signal indicative of a closed status of the tamper loop **604**.

[0046] Thus, FIG. **6** shows a possible implementation for reliably detecting a closed tamper loop. The "closed"-status of the tamper loop **604** is verified by checking if the current received at tamper loop pin **2** is the same (within tolerance ranges) as the current transmitted at tamper loop pin **1**. High disturbances at the tamper loop **604** may cause an alteration of the received current and therefore a "false detection". This risk can be mitigated by increasing the tamper measurement current when a strong field is available and by consequently decreasing the relative amount of disturbance current caused by the RF field.

[0047] FIG. **7** shows a further illustrative embodiment of a tamper detection device **700**. In particular, FIG. **7** shows a detailed implementation of the embodiment shown in FIG. **3**C. The tamper detection device **700** comprises an RFID chip **702** which is operatively coupled to a chip antenna **706** (i.e., an RF antenna) through antenna pins. Furthermore, the tamper detection device **700** comprises a tamper loop **704** which is operatively coupled to the RFID chip **702** through tamper loop pins. In particular, the tamper loop **704** is coupled to a tamper block **710** (i.e., a tamper measurement block). Furthermore, the chip antenna **706** is coupled to a field strength detection unit **708** of the RFID chip **702**. The tamper block **710** comprises a bit stream generation unit **718** which is operatively coupled to the field strength detection unit **708**. Furthermore, the tamper block **710** comprises a current transmitter **714**, a current receiver **716** and a comparator **712**. It is noted that, instead of a current, also a voltage may be used as the measurement signal. In operation, the tamper block **710** may output a tamper measurement signal to be processed by one or more digital components (not shown) of the RFID chip **702**. Furthermore, the field strength detection unit **708** may detect the strength of the RF field present on the chip antenna **706**. If the field strength exceeds a predefined threshold, the bit stream generation unit **718** generates a bit stream and the transmitter **714** transmits a tamper measurement signal having a

complex waveform that represents said bit stream through the tamper loop **704**. The comparator **712** compares the bit stream output by the bit stream generation unit **718** with the waveform of the current received by the receiver **716**. If the waveform of the received current substantially matches the bit stream, the comparator **712** outputs a tamper measurement signal indicative of a closed status of the tamper loop **704**.

[0048] FIG. **8** shows a relationship **800** between tamper loop measurement current and time in the embodiment shown in FIG. **7**. It can be seen that if the field strength exceeds a predefined threshold (i.e., H_{reader} is high), the bit stream generation unit **718** generates a bit stream and the transmitter **714** transmits a tamper measurement signal having a complex waveform that represents said bit stream through the tamper loop **704**. If the field strength does not exceed said threshold (i.e. H_{reader} is low), then a weak constant current is sent through the tamper loop **704**.

[0049] Thus, in one or more embodiments, the tamper measurement unit is configured to change the waveform of the tamper measurement signal in response to a change of the power level. In this way, an open tamper loop can be detected in a more reliable manner. In particular, in case of an open tamper loop, it is very unlikely that distortions from the field cause the same waveform at the receiver part of the tamper measurement circuit than the waveform that is sent by the transmitter part. In one or more embodiments, the waveform of the tamper measurement signal is a complex waveform if the power level exceeds a predefined threshold. On the other hand, if the power level does not exceed said threshold, the waveform of the tamper measurement signal may be a simple waveform. Thus, another implementation option to obtain a robust tamper measurement is to send more complex waveforms over the tamper loop when a stronger field is available, for example. This implementation may prevent false non-detections when the field is sufficiently strong to allow digital patterns to be sent. For example, for a weak RF field (i.e., a field whose strength is below a threshold defined by a given application) the tamper measurement current may be constant, while for a stronger RF field an additional functionality is switched on that allows sending and receiving a digital pattern. In a practical and efficient implementation, the complex waveform represents a bit stream. In short, not only the strength or magnitude of the tamper measurement current, but also its wave shape (i.e., waveform) can be made dependent on the power level.

[0050] FIG. **7** shows a possible implementation of such embodiments. When the field strength is low, then a simple tamper loop measurement can be done such as sending a weak constant current through the tamper loop **704**. When the field strength is sufficiently high, then additional power-consuming circuitry (i.e. the bit stream generation unit **718** and the comparator **712**) can be switched on that sends a digital bit stream through the loop **704** and checks if the sent data is received correctly. A correct reception is then a reliable indicator of a closed tamper loop **704**. If the loop **704** is open, then it is very unlikely that the disturbances caused by the field are causing the same bit stream at the tamper measurement receiver **716** than the one that is sent by the transmitter **714**. Such an implementation may therefore avoid false non-detections.

[0051] The above-described embodiments are, among others, based on the insight that the following relationship exists between the strength of the RF field and the need for disturbance immunity. If the field is weak, then the chip supply will not be strong, so a tamper measurement should be power-economic. Such a tamper measurement is not robust against disturbances caused by the field. However, this is anyhow not required as the disturbances caused by the field are low. If the field is strong, then the chip supply will be strong, so it will be possible to perform a power-consuming tamper measurement. Therefore the tamper measurement is robust against the disturbances that are caused by the strong field.

[0052] It is noted that the embodiments above have been described with reference to different subject-matters. In particular, some embodiments may have been described with reference to method-type claims whereas other embodiments may have been described with reference to device-type claims. However, a person skilled in the art will gather from the above that, unless otherwise indicated, in addition to any combination of features belonging to one type of subject-matter also any combination of features relating to different subject-matters, in particular a combination of features of the method-type claims and features of the device-type claims, is considered to be disclosed with this document.

[0053] Furthermore, it is noted that the drawings are schematic. In different drawings, similar or identical elements are provided with the same reference signs. Furthermore, it is noted that in an effort to provide a concise description of the illustrative embodiments, implementation details which fall into the customary practice of the skilled person may not have been described. It should be appreciated that in the development of any such implementation, as in any engineering or design project, numerous implementation-specific decisions must be made in order to achieve the developers' specific goals, such as compliance with system-related and business-related constraints, which may vary from one implementation to another. Moreover, it should be appreciated that such a development effort might be complex and time consuming, but would nevertheless be a routine undertaking of design, fabrication, and manufacture for those of ordinary skill.

[0054] Finally, it is noted that the skilled person will be able to design many alternative embodiments without departing from the scope of the appended claims. In the claims, any reference sign placed between parentheses shall not be construed as limiting the claim. The word "comprise(s)" or "comprising" does not exclude the presence of elements or steps other than those listed in a claim. The word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. Measures recited in the claims may be implemented by means of hardware comprising several distinct elements and/or by means of a suitably programmed processor. In a device claim enumerating several means, several of these means may be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

LIST OF REFERENCE SIGNS

[0055] **100** tamper detection device
[0056] **102** integrated circuit
[0057] **104** antenna
[0058] **106** detection wire

[0059] **108** pull linkage
[0060] **110** detailed view of integrated circuit
[0061] **200** RFID system
[0062] **202** RFID chip
[0063] **204** tamper loop
[0064] **206** chip antenna
[0065] **208** reader
[0066] **210** reader antenna
[0067] **212** RFID system
[0068] **214** RFID chip
[0069] **216** tamper loop
[0070] **218** chip antenna
[0071] **220** reader
[0072] **222** reader antenna
[0073] **300** tamper detection device
[0074] **302** RFID chip
[0075] **304** tamper loop
[0076] **306** antenna
[0077] **308** field strength detection
[0078] **310** tamper measurement block
[0079] **312** transmitter
[0080] **314** receiver
[0081] **316** tamper detection device
[0082] **318** RFID chip
[0083] **320** tamper loop
[0084] **322** tamper measurement block
[0085] **324** transmitter
[0086] **326** receiver
[0087] **328** tamper detection device
[0088] **330** RFID chip
[0089] **332** tamper loop
[0090] **334** tamper measurement block
[0091] **336** bit stream transmitter
[0092] **338** bit stream receiver
[0093] **400** tamper detection device
[0094] **402** RFID chip
[0095] **404** tamper loop
[0096] **406** chip antenna
[0097] **408** front-end
[0098] **410** tamper block
[0099] **412** receive buffer
[0100] **414** voltage-controlled current source
[0101] **416** limiter control circuit
[0102] **418** rectifier and power regulator
[0103] **500** relationship between limiter activity and tamper loop measurement current
[0104] **502** limiter activity
[0105] **504** tamper loop measurement current
[0106] **600** tamper detection device
[0107] **602** RFID chip
[0108] **604** tamper loop
[0109] **606** chip antenna
[0110] **608** front-end
[0111] **610** tamper block
[0112] **612** comparator
[0113] **614** voltage-controlled current source (transmitter)
[0114] **616** limiter control circuit
[0115] **618** rectifier and power regulator
[0116] **620** current measurement (receiver)
[0117] **700** tamper detection device
[0118] **702** RFID chip
[0119] **704** tamper loop
[0120] **706** chip antenna
[0121] **708** field strength detection
[0122] **710** tamper block
[0123] **712** comparator
[0124] **714** transmitter
[0125] **716** receiver
[0126] **718** bit stream generation
[0127] **800** relationship between tamper loop measurement current and time

1. An electronic tamper detection device comprising a radio frequency antenna, a tamper loop, a power level determination unit and a tamper measurement unit, wherein:
- the power level determination unit is configured to determine a power level of the tamper detection device;
- the tamper measurement unit is configured to generate a measurement signal and to transmit said measurement signal through the tamper loop;
- the tamper measurement unit is further configured to adapt the measurement signal in dependence on the power level.

2. The device of claim **1**, wherein the power level corresponds to the strength of a radio frequency field present on the radio frequency antenna and the power level determination unit is configured to detect said strength, or wherein the power level corresponds to a chip supply voltage and the power level determination unit is configured to monitor said chip supply voltage.

3. The device of claim **1**, wherein the tamper measurement unit is further configured to receive the measurement signal from the tamper loop or to receive a signal derived from the measurement signal from the tamper loop.

4. The device of claim **1**, wherein the tamper measurement unit is configured to change the magnitude of the measurement signal in response to a change of the power level.

5. The device of claim **4**, wherein the field strength detection unit comprises a limiter control circuit operatively coupled to the tamper measurement unit, and wherein the tamper measurement unit is configured to change the magnitude of the measurement signal under control of the limiter control circuit.

6. The device of claim **1**, wherein the tamper measurement unit is configured to change the waveform of the measurement signal in response to a change of the power level.

7. The device of claim **6**, wherein the waveform of the measurement signal is a complex waveform, in particular a waveform that represents a bit stream, if the power level exceeds a predefined threshold.

8. The device of claim **6**, wherein the waveform of the measurement signal represents a constant current if the power level does not exceed said threshold.

9. The device of claim **1**, being an RFID-enabled tamper detection device.

10. The device of claim **1**, being a BLE-enabled tamper detection device.

11. The device of claim **1**, wherein the tamper measurement unit comprises a voltage-controlled current source, a current-controlled current source, a current-controlled voltage source, or a voltage-controlled voltage source.

12. The device of claim **1**, wherein the tamper loop is a conductive wire.

13. The device of claim **1**, wherein the tamper measurement unit is configured to generate a tamper measurement signal for further processing by a digital circuit.

14. A tamper detection method using an electronic tamper detection device, wherein said device comprises a radio frequency antenna, a tamper loop, a power level determination unit and a tamper measurement unit, the method comprising:

the power level determination unit determines a power level of the tamper detection device;

the tamper measurement unit generates a measurement signal and transmits said measurement signal through the tamper loop;

the tamper measurement unit adapts the measurement signal in dependence on the power level.

15. A non-transitory computer-readable storage medium comprising instructions which, when executed by a processing unit, carry out or control the method of claim **14**.

* * * * *